(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 849 657 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
24.06.1998 Bulletin 1998/26

(51) Int Cl.[6]: **G06F 1/00**, G06F 12/14

(21) Application number: **97309454.3**

(22) Date of filing: **24.11.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **18.12.1996 GB 9626241**

(71) Applicant: **NCR International, Inc.**
Dayton, Ohio 45479 (US)

(72) Inventor: **Saunders, Keith A.**
Dundee, Scotland DD2 5RR (GB)

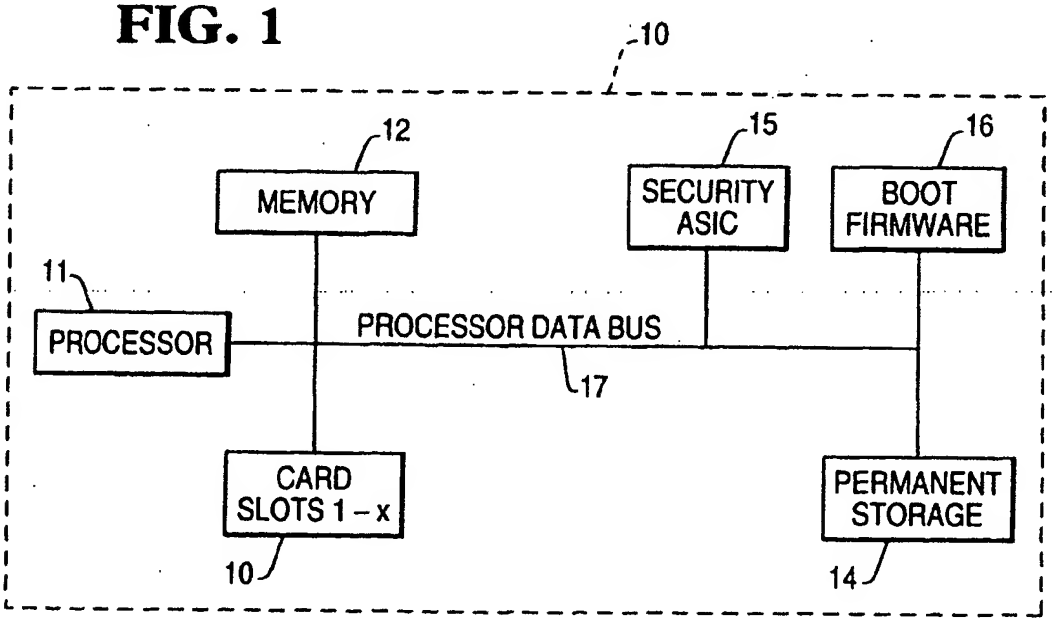
(74) Representative: **Irish, Vivien Elizabeth et al**
International IP Department,
NCR Limited,
206 Marylebone Road
London NW1 6LY (GB)

(54) Secure data processing method and system

(57) A secure data processing system comprises a central processor unit (11), memory (12) and a security circuit (15) in the form of an application specific integrated circuit. The security circuit has a cryptographic engine (19) and a cryptographic key store (18).

The cryptographic engine operates on the contents of the cryptographic key store to generate a digital signature. Means are provided to generate a digital signature from a software or hardware component to be checked for authenticity and to compare the digital signature from the component with the generated digital signature. An indication of the authenticity of the component is generated as a result of the comparison. The components of the system that can be checked include the boot firmware (16) for the system, the operating system and plug-in cards (13) for the system.

FIG. 1



EP 0 849 657 A1

Description

The present invention concerns a secure data processing method and system and is of particular application to a financial terminal.

In a data processing system it is usual to provide a programmable central processor unit, memory and other software and hardware components. It is desirable to provide a software and hardware environment where the user or operator of the system can trust all of the software and hardware components of the system. To achieve this objective some means has to be provided to decide whether the components of the system have been compromised either at initial installation of the components or at a later stage when new or upgraded components are introduced to the system.

For a data processing system including a programmable central processor unit it is important to authenticate the operating system of the central processor unit. If plug-in cards are used to provide upgrades to the functionality of the system it is also important to authenticate these plug-in cards. The means to authenticate the components of the data processing system must be such as to provide security for the authentication process itself if the authentication process is to be reliable in detecting any compromise of the components of the system.

It is therefore an object of the present invention to provide an effective method and system for testing one or more components of a data processing system in order to determine the authenticity of the tested component or components.

According to the present invention there is provided a method of determining the authenticity of one or more system components of a data processing system which also includes a programmable central processor unit, memory, a security circuit having a cryptographic engine, and a cryptographic key store, the method comprising the steps of entering one or more keys into the cryptographic key store, operating on the contents of the cryptographic key store by means of the cryptographic engine to generate a digital signature referenced to a component of the system to be authenticated, generating a digital signature from the component to be authenticated, and providing an indication of authenticity by comparing the digital signature generated by the cryptographic engine with that generated from the component to be authenticated.

Further according to the present invention there is provided a data processing system including one or more components to be checked for authenticity, a programmable central processing unit, memory and a security circuit having a cryptographic engine and a cryptographic key store for storing one or more cryptographic keys, the cryptographic engine being adapted to operate on the contents of the cryptographic key store to generate a digital signature referenced to a component of the system to be checked for authenticity, and means being provided to generate a digital signature from the component to be checked for authenticity and to provide an indication of authenticity by comparing the digital signature generated by the cryptographic engine with that generated from the component to be authenticated.

The invention will now be described, by way of example, with reference to the accompanying drawings in which:

Figure 1 shows a block diagram of a data processing system according to the present invention,

Figure 2 shows detail of a security circuit included in the system of Figure 1,

Figure 3 shows a flow diagram of the operation of the system of Figures 1 and 2, and

Figure 4 shows a flow diagram relating to the update of cryptographic keys used in the system of Figures 1 and 2.

Referring first to Figure 1, there is shown a data processing system 10 which may be an automatic teller system or a personal computer system. The system 10 has a central processor unit 11, a memory 12, provision for additional plug-in cards 13, permanent storage 14, a security circuit 15 in the form of an application specific integrated circuit (ASIC) and boot firmware 16. The components of the data processing system 10 are linked by means of a processor data bus 17 in conventional manner well understood by those skilled in the art. In addition the system runs under an operating system (OS) in a manner well understood in the art.

The security circuit 15 is shown in greater detail in Figure 2. Referring now to Figure 2, the circuit 15 includes a cryptographic key and password store 18, a cryptographic engine 19, a store 20 for a digital signature, control and interface firmware 21 and an I/O bus 22 communicating with the system bus 17. The cryptographic engine 19 supports both symmetric and asymmetric algorithms. The control and interfacing firmware 21 is designed to perform the initial start-up of the data processing system.

Means (not shown) are provided to allow the operator of the system to input keys and passwords into the security circuit 15. All the keys stored in the storage 18 are password protected, with the password defined (and changeable) by input from the user of the system. A key can therefore only be altered if the corresponding password is known and entered by the user.

The keys in the stor 18 are present to allow system components including firmware components and software components to be authenticated. The components to be authenticated in the system of Figure 1 include the operating

system (OS), th firmware on the plug-in cards 13, and the boot firmware 16. The invention may be applied to a system which has either more or fewer system components to be authenticated than the system depicted in Figure 1. For example a simpler system may not provide for the plug-in cards 13 and in this case provision may not be required to authenticate such cards.

Each of the components of the system which are to be authenticated includes a digital signature which is embedded in the firmware of the component. The digital signature is embedded at a predefined location and is created by the supplier of the component as part of the manufacturing process. The algorithm for generating the digital signature uses an asymmetric key pair, with the vendor supplier keeping the private key securely and distributing the public key with the component to be authenticated. The public key is entered into the circuit 15 when the component is installed into the data processing system 10.

The creator of each of the cryptographic keys entered into the circuit 15 will depend on the source of the component to which the keys relate. The keys may be symmetric or asymmetric and validate the respective components of the system according to the cryptographic process determined within the security circuit 15. The authentication process is tamper proof by reason of the fact that the process is contained within the security ASIC 15 and it is not feasible to alter the contents of this ASIC. The security system can not be disabled.

A number of keys are pre-defined as shown in the following Table 1:

TABLE 1

Key Name	Type	Use	Creator
Boot	Asymmetric	Validation of boot firmware by ASIC 15	ASIC
Cards (1-x)	Asymmetric	Validation of firmware of cards (1-x)	The creator of boot firmware The creator of the card firmware for cards (1-x)
OS	Symmetric	Validation of operating system boot Automatically generated by the ASIC (15).	

The process of starting up the data processing system of Figures 1 and 2 is shown in the flow diagram of Figure 3. Referring now to Figure 3, the power on step 23 is followed by processor start-up step 24 and the execution at step 25 of the initial code of the ASIC 15. A decision is taken at step 26 whether the boot key has been loaded and validation of the boot PROM 16 takes place in step 27 either directly or via step 28 if the boot key has to be entered. The process of validation in step 27 comprises the generation within the ASIC 15 of the expected digital signature using the 'boot' key. The generated digital signature is then compared to the actual digital signature from the boot PROM 16 and an indication is generated in step 29 whether the boot PROM is valid. If not valid, the process in Figure 3 is stopped.

If the boot PROM 16 is validated, the process continues through the step 30 to execute the boot PROM and then begins in step 31 to operate on each of the plug-in cards 13. In the flow diagram of Figure 3, each card x (where x is the number of each card taken in turn) is checked by determining in step 32 if the corresponding card key has been entered in the ASIC 15 and validation proceeds in step 33 either directly if th key has been entered, or via the step 34 if the key has still to be entered. Validation of each plug-in card 13 is achieved by comparison of th digital signature generated for that card by the cryptographic engine 19 with the digital signature embedded in the card using th appropriate 'card x' key (where x is the number of each card taken in turn. An indication is generated in step 35 whether the card is valid. If the card is valid, th card initial code is executed in step 36.

If there are succeeding cards to be validated, this is determined in step 37 and the validation of all the cards

continues until all have been validated. Following validation of the cards, the boot record is validated in step 38 and an indication provided in step 39 if the boot record is valid. The process of validation in step 38 is performed by generating a digital signature for the operating system boot using the 'OS' key and comparing this against the digital signature stored in the digital signature store 20. If the boot record is valid, the boot record code is executed in step 40 and the system is running.

Referring now to Figure 4, the method of updating the keys will be described. to commence an operating system or card key update, from step 41, a check is made whether the terminal is running in step 42. If not running, the system is powered up in step 43 and a check made in step 44 whether the system has failed. If yes, an update function key is pressed, a password for the selected key is entered and the new key is entered to arrive at the step 45 where the system starts normally.

If at step 44 the terminal has not failed, the key update program is run in step 46 and the operator of the system selects which key to update in step 47. The password for the selected key is entered at step 48, the new key is entered at step 49 and the system is powered down in step 50. The system component (either a card 13 or the BIOS) is replaced at step 51 and the terminal powered up again at step 52.

If there is a boot record failure as shown in step 53, an update function key is pressed at step 54 and the password for the operating system signature is entered at step 55. This results in the operating system digital signature being re-generated. The operating system operates normally at step 56.

Once the operating system is started, the security is the responsibility of the operating system software. The security ASIC 15 can then provide validation of digitally signed software.

It will be apparent that the system described allows a trusted start up sequence that is required for successfully providing a complete secure system. It is envisaged that the keys could be stored in storage outside the security ASIC 15. For example they could be encrypted under a master key which is held within the security ASIC 15 which would make it impossible to alter or replace the keys.

Claims

1. A method of determining the authenticity of one or more system components of a data processing system which also includes a programmable central processor unit, memory, a security circuit having a cryptographic engine, and a cryptographic key store, characterized by the steps of entering one or more keys into the cryptographic key store, operating on the contents of the cryptographic key store by means of the cryptographic engine to generate a digital signature referenced to a component of the system to be authenticated, generating a digital signature from the component to be authenticated, and providing an indication of authenticity by comparing the digital signature generated by the cryptographic engine with that generated from the component to be authenticated.

2. A method as claimed in claim 1, including the further steps of updating a key in the cryptographic key store by selecting a key to be updated, entering a password for the selected key and entering the updated key.

3. A data processing system (10) including one or more components (13,16) to be checked for authenticity, a programmable central processing unit, (11) and a memory (12), characterized by a security circuit (15) having a cryptographic engine (19) and a cryptographic key store (18) for storing one or more cryptographic keys, the cryptographic engine being adapted to operate on the contents of the cryptographic key store to generate a digital signature referenced to a component to be checked for authenticity, and means being provided to generate a digital signature from the component to be checked for authenticity and to provide an indication of authenticity by comparing the digital signature generated by the cryptographic engine with that generated from the component to be authenticated.

4. A system as claimed in claim 3, wherein a component to be checked for authenticity comprises boot firmware (16) for the system.

5. A system as claimed in claim 3 or 4, wherein a component to be checked for authenticity comprises an operating system.

6. A system as claimed in claim 3, 4 or 5, wherein a component to be checked for authenticity comprises a plug-in card (13).

7. A system as claimed in claim 3, 4, 5 or 6, wherein the security circuit (15) has means (18) for storing passwords to control the entry of cryptographic keys into the cryptographic key store.

8. A system as claimed in any one of claims 3 to 7, wherein the security circuit (18) comprises an integrated circuit.

FIG. 1

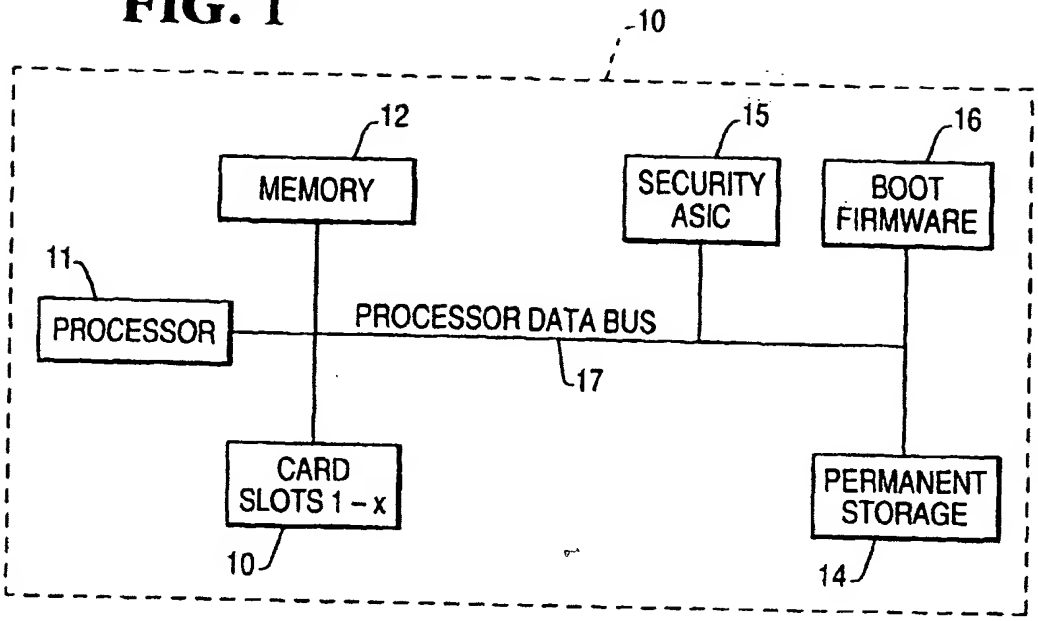

10
12
MEMORY
15
SECURITY ASIC
16
BOOT FIRMWARE
11
PROCESSOR
PROCESSOR DATA BUS
17
CARD SLOTS 1 – x
10
PERMANENT STORAGE
14

FIG. 2

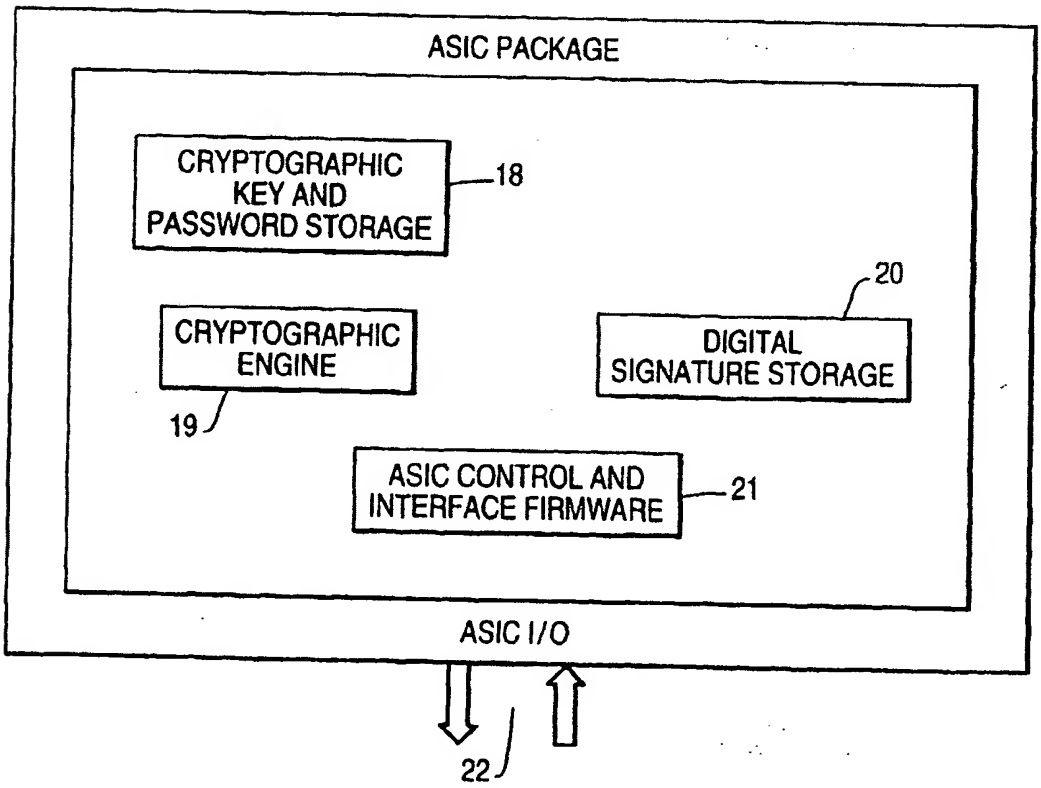

ASIC PACKAGE
CRYPTOGRAPHIC KEY AND PASSWORD STORAGE
18
20
CRYPTOGRAPHIC ENGINE
19
DIGITAL SIGNATURE STORAGE
ASIC CONTROL AND INTERFACE FIRMWARE
21
ASIC I/O
22

FIG. 3

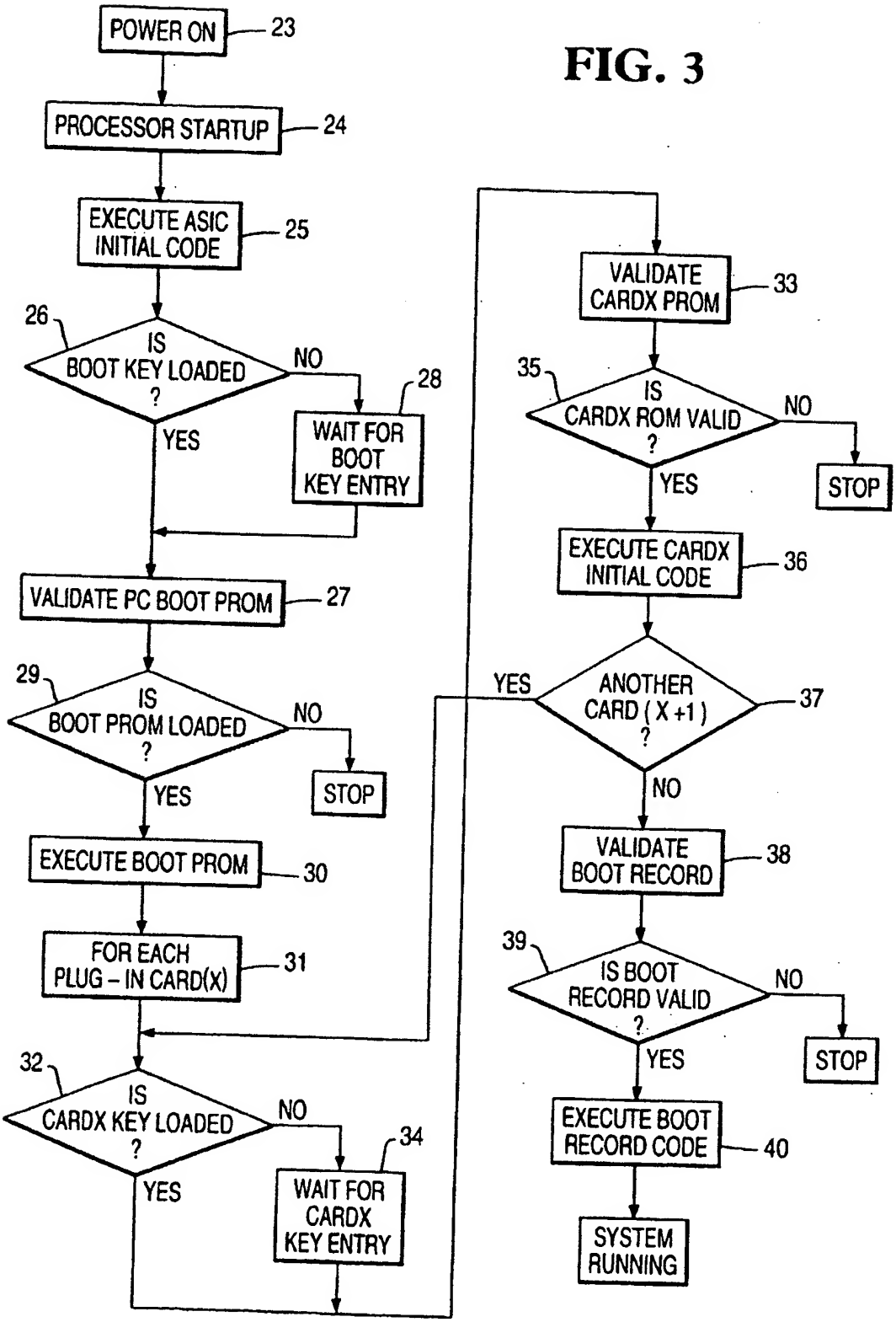
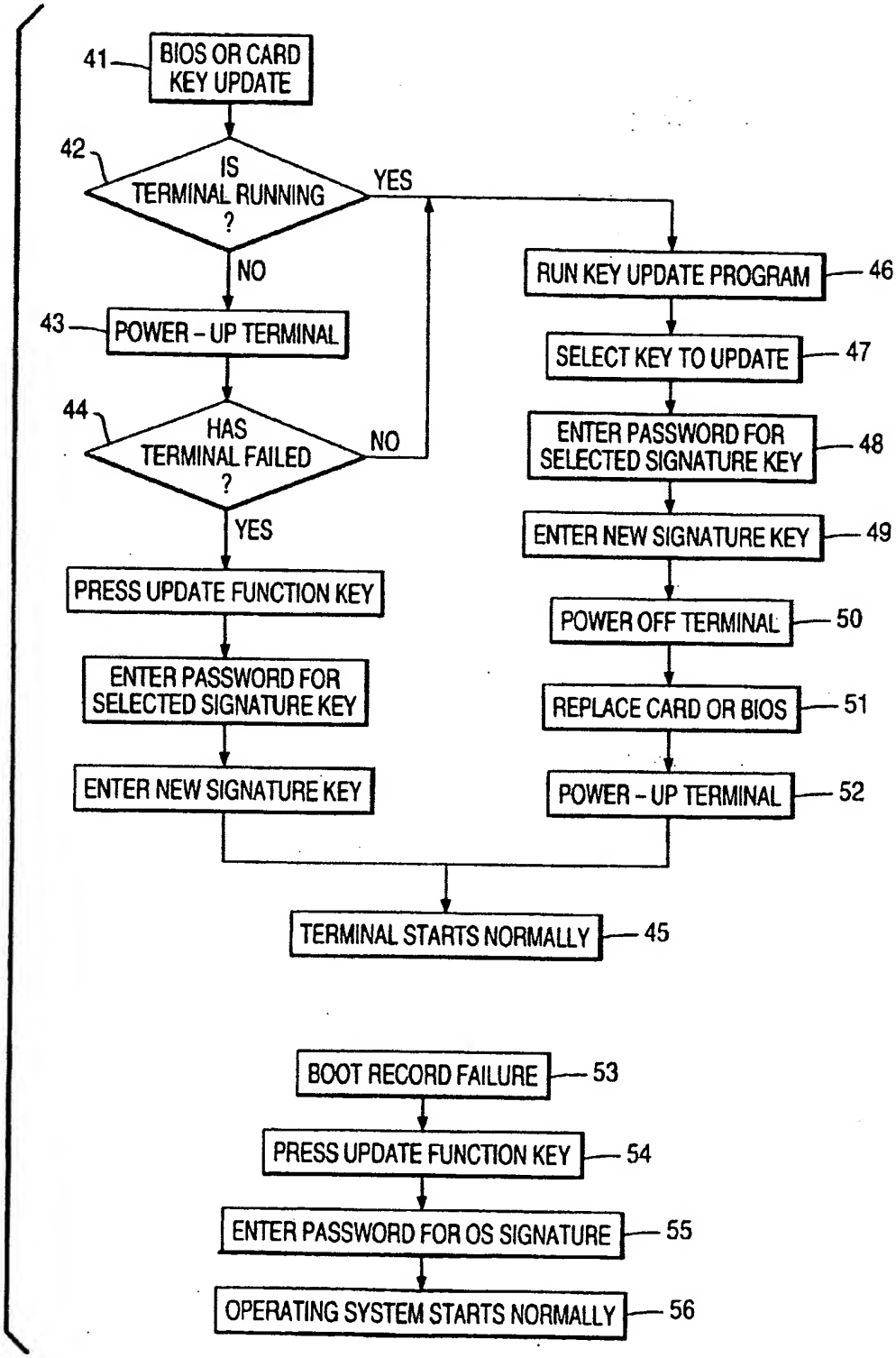

POWER ON
23
PROCESSOR STARTUP
24
EXECUTE ASIC INITIAL CODE
25
26
IS BOOT KEY LOADED ?
NO
28
WAIT FOR BOOT KEY ENTRY
YES
VALIDATE PC BOOT PROM
27
29
IS BOOT PROM LOADED ?
NO
STOP
YES
EXECUTE BOOT PROM
30
FOR EACH PLUG – IN CARD(X)
31
32
IS CARDX KEY LOADED ?
NO
34
WAIT FOR CARDX KEY ENTRY
YES
VALIDATE CARDX PROM
33
35
IS CARDX ROM VALID ?
NO
STOP
YES
EXECUTE CARDX INITIAL CODE
36
ANOTHER CARD (X +1) ?
37
YES
NO
VALIDATE BOOT RECORD
38
39
IS BOOT RECORD VALID ?
NO
STOP
YES
EXECUTE BOOT RECORD CODE
40
SYSTEM RUNNING

FIG. 4


41
BIOS OR CARD KEY UPDATE
42
IS TERMINAL RUNNING ?
YES
NO
43
POWER - UP TERMINAL
44
HAS TERMINAL FAILED ?
NO
YES
PRESS UPDATE FUNCTION KEY
ENTER PASSWORD FOR SELECTED SIGNATURE KEY
ENTER NEW SIGNATURE KEY
RUN KEY UPDATE PROGRAM
46
SELECT KEY TO UPDATE
47
ENTER PASSWORD FOR SELECTED SIGNATURE KEY
48
ENTER NEW SIGNATURE KEY
49
POWER OFF TERMINAL
50
REPLACE CARD OR BIOS
51
POWER - UP TERMINAL
52
TERMINAL STARTS NORMALLY
45
BOOT RECORD FAILURE
53
PRESS UPDATE FUNCTION KEY
54
ENTER PASSWORD FOR OS SIGNATURE
55
OPERATING SYSTEM STARTS NORMALLY
56

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 30 9454

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	US 5 473 692 A (DAVIS DEREK L) * abstract; figures 5,6 * * column 2, line 58 - column 3, line 31 * * column 7, line 23 - column 8, line 22 *	1,3-6,8	G06F1/00 G06F12/14
Y	US 5 343 527 A (MOORE JAMES W) * the whole document *	1,3-6,8	
Y	US 5 224 160 A (PAULINI WERNER ET AL) * abstract; figures 3,6 * * column 2, line 1 - column 3, line 32 *	4,5	
A	KRUSE D: "GUARDING THE OPERATING SYSTEM" SIEMENS MAGAZINE OF COMPUTERS & COMMUNICATIONS, (COM), vol. 14, no. 5, September 1986, pages 14-16, XP000611029	2,7	
A	EP 0 707 270 A (IBM)		

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	26 March 1998	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)